UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

John Doe, *on behalf of himself and all others similarly situated*, Plaintiff, v. SSM Health Care Corporation d/b/a SSM Health, Defendant.	Case No. 4:23-cv-12 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff John Doe is a former patient of SSM Health Care Corporation d/b/a SSM Health ("SSM Health" or "Defendant"), who brings this class action against Defendant in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions, his counsels' investigation, and, upon information and belief, as to all other matters, as follows:

1. This case arises from Defendant's intentional, reckless, and negligent disclosure of Plaintiff's and Class Members' confidential and private medical information to Meta Platforms, Inc., d/b/a Meta ("Facebook").

2. Defendant's website (https://www.ssmhealth.com/) (hereinafter, the "Website") contain a well-known Facebook tracking pixel (the "Pixel" or "Facebook Pixel") that secretly enables the unauthorized transmission and disclosure of Plaintiff's and Class Members' confidential medical information to Facebook.

3. In doing so, Defendant unlawfully discloses Plaintiff's and Class Members'

personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") contained in the confidential communications to Facebook.

4. When an individual visits the Defendant's website, the Facebook Pixel causes that individual's unique and persistent Facebook ID ("FID") to be transmitted alongside other Private Information that is sent to Facebook.

5. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[1] as they interact with a website. The Facebook Pixel can be used to track an array of actions and events, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and what text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box). The Facebook Pixel is programmable, meaning that the Defendant controls which events are tracked and transmitted to Facebook.

6. Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data for marketing purposes in an effort to bolster its profits.

7. Operating as designed and as implemented by Defendant, the Pixel allowed the Private Information that Plaintiff and Class Members submitted to it to be unlawfully disclosed to Facebook.

8. For example, when Plaintiff or a Class Member accessed Defendant's website, the website visitor's internet browser automatically and surreptitiously sent their Private Information to Facebook as they navigated, interacted, and communicated with Defendant's website. This

[1] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 14, 2022)

occurred on every web page hosting the Facebook Pixel because the underlying software instructs the website visitor's browser to communicate and transmit information to Facebook.

9. The information sent to Facebook includes Private Information that Plaintiff and Class Members submitted to Defendant's website, including for example, the type and date of a medical appointment and physician. Such Private Information would allow a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or HIV.

10. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on the Private Information submitted to Defendant's website.

11. For instance, Plaintiff submitted medical information on the Website and used the Find-A-Doctor feature to find a psychologist, psychiatrist, and primary care provider. He also used the Website to find medical testing options.

12. Shortly thereafter, Plaintiff started receiving advertisements to his Facebook page ("Facebook Advertisements") related to the medical information that he disclosed via the Website.

13. The Facebook Advertisements seek to provide the same relief as the prescription medication that Plaintiff communicated to Defendant via the Website. In other words, the Facebook Advertisement was targeted towards Plaintiff based on the Private Information Plaintiff communicated to Defendant, who in turn, disclosed to Facebook.

14. Based upon the Facebook Pixel configuration on Defendant's website, Defendant disclosed Plaintiff's medical information to Facebook, who, in turn, sold Plaintiff's Private Information to third parties for monetary gain.

15. Defendant regularly encourages Plaintiff and Class Members to use its digital tools, including the Website, to receive healthcare services. Plaintiff and Class Members provided their Private Information through Defendant's website with the reasonable understanding that Defendant would secure and maintain any PII and PHI as confidential.

16. At all times that Plaintiff and Class Members visited and utilized Defendant's website, they had a reasonable expectation of privacy in the Private Information collected through Defendant's website, including that it would remain secure and protected and only utilized for medical purposes.

17. Plaintiff and Class Members provided Private Information to Defendant in order to receive medical services rendered and with the reasonable expectation that Defendant would protect their Private Information. Plaintiff and Class Members relied on Defendant to secure and protect the Private Information and not disclose it to unauthorized third parties without their knowledge or consent.

18. Defendant further made expressed and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

19. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members communications and medical information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

20. Defendant, however, failed in its obligations and promises by utilizing the Facebook Pixel, described below, on its Website knowing that such technology would transmit

and share Plaintiff's and Class Members' Private Information with unauthorized third parties.

21. The exposed Private Information of Plaintiff and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties can often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

22. While Defendant willfully and intentionally incorporated the tracking Pixel into its website, Defendant has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications via the website with Facebook. As a result, Plaintiff and Class Members were unaware that their PII and PHI were being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website.

23. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their PII and PHI to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' PII and PHI through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its website to maintain the confidentiality and integrity of patient PII and PHI.

24. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (v) the

continued and ongoing risk to their Private Information.

25. Plaintiff seek to remedy these harms and bring causes of action for (1) Invasion of Privacy; (2) violations of Mo. Rev. Stat. § 407.010 *et seq.*; (3) unjust enrichment; (4) breach of implied contract; (5) violations of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) - unauthorized interception, use, and disclosure; (6) violations of ECPA, 18 U.S.C. § 2511(3)(a) - unauthorized interception, use, and disclosure; (7) violations of Title II of the ECPA, 18 U.S.C. § 2702, *et seq*., - Stored Communications Act; (8) violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq*.; and (9) breach of confidence.

PARTIES

26. Plaintiff is a natural person and citizen of Missouri, residing in St. Louis, Missouri (St. Louis County) where he intends to remain. On numerous occasions, from 2018 to present, Plaintiff accessed the Website on his mobile device and/or computer. Plaintiff used the Website to find and obtain a physician specialized in treating Attention Deficit Hyperactivity Disorder, and he communicated information about his medical condition, treatments, and symptoms via the Website. Pursuant to the systematic process described herein, Plaintiff's communications were disclosed to Facebook, and this data included his personally identifiable information, protected health information, and related confidential information. Defendant assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's PII and PHI.

27. Defendant SSM Health is a 501(c)(3) non-profit corporation organized under, and governed by, Missouri law. SSM Health is headquartered at 3 City Place Drive, Ste. 700, St. Louis, Missouri. SSM Health operates care delivery sites in Illinois, Missouri, Oklahoma, and Wisconsin,

including 23 hospitals, more than 300 physician offices and other outpatient and virtual care services, 13 post-acute facilities, comprehensive home care and hospice services, a pharmacy benefit company, a health insurance company and an accountable care organization. It is one of the largest employers in every community it serves.[2]

28. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 "HIPAA")

JURISDICTION & VENUE

29. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

30. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (28 U.S.C. § 2511, *et seq.*, and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq*).

31. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

32. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

Defendant Improperly Disclosed Plaintiff's and Class Members' Private Information

[2] https://www.ssmhealth.com/resources/about (last visited: December 19, 2022).

33. Defendant encourages and promotes Plaintiff and Class Members use of its digital healthcare platforms, the Website, with the goal of increasing profitability.

34. To accomplish this, upon information and belief, Defendant utilized Facebook advertisements and intentionally installed the Pixel on its website. The Pixel is a piece of code that Defendant used to secretly track patients by recording their activity and experiences on Defendant's Website and related electronic platforms.[3]

35. Through seeking and using Defendant's services as a medical provider, including the Website, Plaintiff's and Class Members' Private Information was intercepted in real time and disseminated to Facebook, and potentially to other third parties, via the Pixel that Defendant secretly installed on its website.

36. Plaintiff and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook or that Defendant was tracking their every movement and disclosing the same to Facebook when they entered highly sensitive information on Defendant's Website and.

37. Defendant did not disclose to or warn Plaintiff or Class Members that: (1) Defendant used their confidential electronic medical communications for marketing purposes; or (2) tracked and disseminated their Private Information via the Facebook Pixel.

38. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information.

39. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiff's and Class Members' status as medical patients;

[3] *Id.*

b. Plaintiff's and Class Members' communications with Defendant through its Website;

c. Plaintiff's and Class Members' medical appointments, location of treatments, specific medical providers, and specific medical conditions and treatments;

d. Plaintiff's and Class Members' personal identifying information, including their unique and persistent Facebook User ID ("FID"); and

e. Other sensitive and medical information contained within Defendant's website.

40. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent

Operation Source Code

41. Web browsers are software applications that allow consumers to exchange electronic communications over the internet.

42. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with Internet users via their web browsers.

43. The set of instructions that commands the browser is called the source code.

44. Source code may also command a web browser to send data transmissions to third parties via pixels or web bugs, tiny 1x1 invisible GIF files that effectively open a spying window through which a website funnels data about users and their actions to third parties.

45. The third parties to whom the website transmits data through pixels or web bugs do

not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes.

46. The web bugs are tiny and camouflaged to purposefully remain invisible to the user.

47. Thus, without any knowledge, authorization, or action by a user, a website developer like Defendant can use its source code to commandeer the user's computing device, causing the device in this case to contemporaneously and invisibly re-direct the users' Private Information to third parties.

The Facebook Pixel

48. The Defendant secretly deployed the Pixel on its website in violation of its common law, contractual, statutory, and regulatory duties and obligations.

49. The Facebook Pixel, a marketing product, is a "piece of code" that allowed the Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."[4] It also allowed the Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, learn about the website, and decrease advertising and marketing costs.[5]

50. Most importantly, it allowed Defendant and Facebook to secretly track and intercept patients' communications on Defendant's website and patient portal.

Facebook's Platform and its Business Tools

51. Facebook operates the world's largest social media company.

52. In 2021, Facebook generated $117 billion in revenue.[6] Roughly 97% of that came

[4] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022)
[5] *Id.*
[6] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022)

from selling advertising space.[7]

53. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses.

54. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.

55. Facebook then sells advertising space by highlighting its ability to target users.[8] Facebook can target users so effectively because it surveils user activity both on and off its site.[9] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[10] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[11]

56. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

57. Advertisers can also build "Custom Audiences."[12] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[13] With Custom

---

[7] *Id.*
[8] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Nov. 14, 2022).
[9] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022).
[10] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).
[11] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Nov. 14, 2022).
[12] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Nov. 14, 2022).
[13] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).

Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[14] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," including the Facebook Pixel.[15]

58. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[16] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

59. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[17] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers

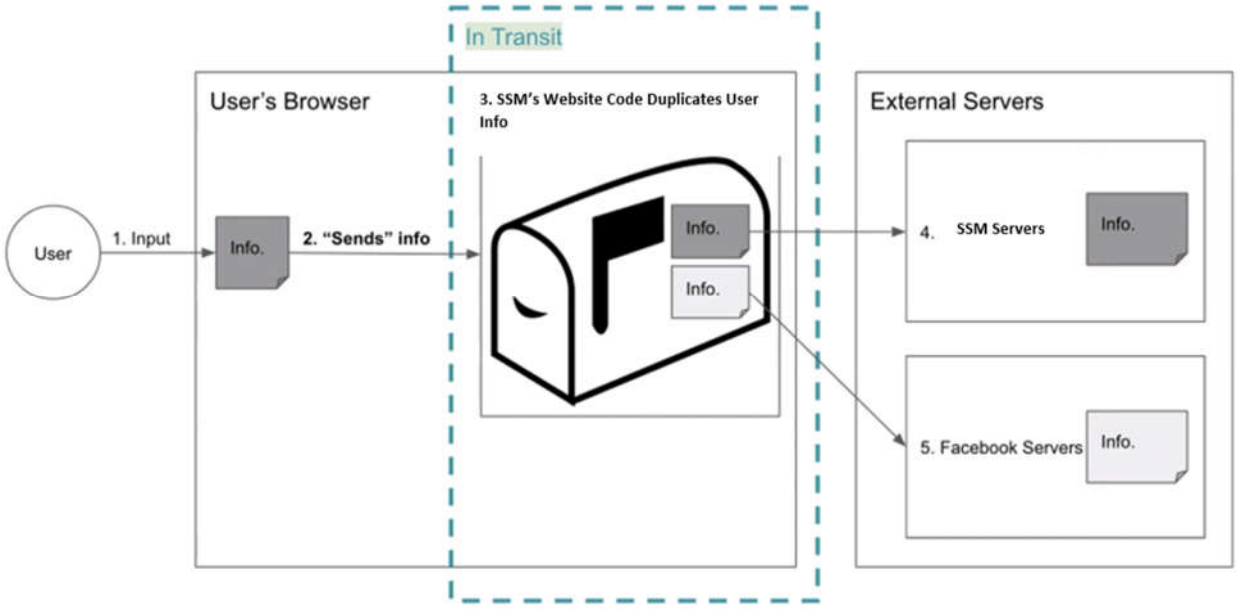
[14] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Nov. 14, 2022).
[15] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Nov. 14, 2022).
[16] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Nov. 14, 2022).
[17] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov. 14, 2022).

can choose, including what content a visitor views or purchases.[18] Advertisers can even create their own tracking parameters by building a "custom event." [19]

60. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their website. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[20] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's websites—Defendant's own code, and Facebook's embedded code.

61. An example illustrates the point. Plaintiff submitted medical information to Defendant via the Website. Because Defendant utilizes the Facebook Pixel, the Website's Source Code, sends a secret set of instructions back to the individual's browser, causing it to secretly duplicate communications with Defendant. As a result, a second and identical set of information is automatically and instantaneously sent to Facebook's servers without the Website visitors' knowledge. The image below illustrates this process:

[18] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Nov. 14, 2022)
[19] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited Nov. 14, 2022)
[20] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

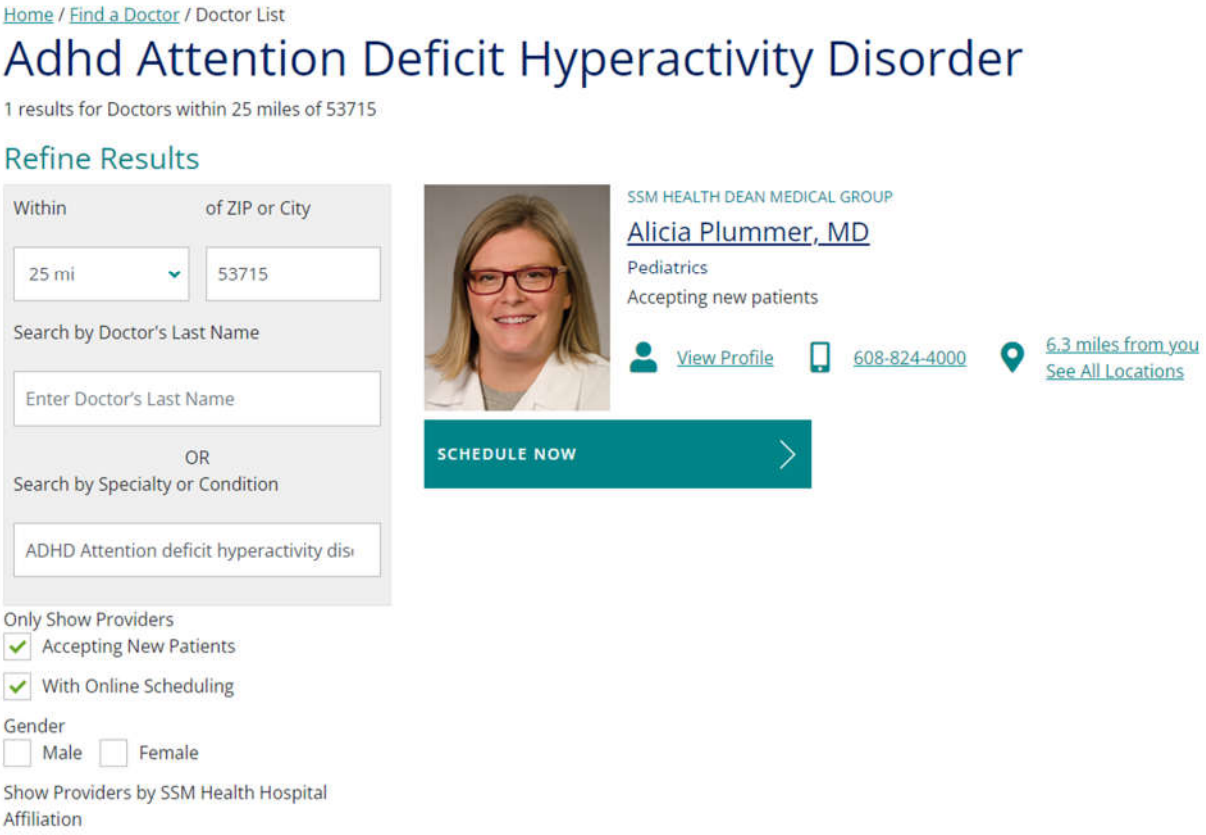


62. This second transmission is sent alongside additional information that transcribes the communication's content and the individual's identity.

63. Consequently, when Plaintiff and Class Members visited Defendant's website and entered their Private Information to Defendant's website, it was transmitted to Facebook, including, but not limited to, appointment type and date, physician selected, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information.

64. For example, the images below demonstrate that, as a patient communicates their health information to the Website, that information is duplicated and sent to Facebook.

65. In the first image the patient has used the Website to locate a doctor specializing in ADHD treatment who is currently accepting new patients, and offering online appointment scheduling services.



66. The next image shows the information that is sent to Facebook when the patient enters their search parameters. The word "PageView" communicates the fact that the user viewed the webpage above, and the URL information (highlighted in yellow below) communicates the fact that the patient used the "find-a-doctor" tool to locate a physician who is "accepting new patients," offers "online-scheduling," and treats "adhd attention deficit hyperactivity disorder." The users' zipcode was also communicated to Facebook.

▼ Request Headers

:authority: www.facebook.com
:method: GET
:path: /tr/?id=533188793867876&ev=PageView&dl=https%3A%2F%2Fwww.ssmhealth.com%2Ffind-a-doctor%2Fdoctorslist%2F
adhd-attention-deficit-hyperactivity-disorder%2Fonline-scheduling%2Faccepting-new-patients%3FIsFromLandingPa
e%3Dtrue%26Zipcode%3D53715%26Radius%3D25%26AcceptingNewPatient%3Dtrue%26OnlineScheduling%3Dtrue%26PageSize%3
20&rl=https%3A%2F%2Fwww.ssmhealth.com%2Ffind-a-doctor&if=false&ts=1672859866763&sw=1920&sh=1080&v=2.9.90&r=s
able&ec=0&o=28&it=1672859866449&coo=false&rqm=GET
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
cookie: sb=G1UJYYwZM-i797zPAJe7wSMo; datr=G1UJYcU6fHxA7S_dXYoksRLp; c_user=150[redacted] xs=13%3A_J9153zJbvWkKg
3A2%3A1672416877%3A-1%3A2663%3A%3AAcVNxbZ1Z077xN2nOKiicGSXbmhu-axDDYXMp7j5uA; fr=0h8pcRNO2Xh8qjCcn.AWWbwJvW
DT9QOB9vzYsF1XMSo.Bjtc-a.3g.AAA.0.0.Bjtc-a.AWU-ORgmOqI
referer: https://www.ssmhealth.com/
sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: cross-site
user-agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safar
i/537.36

67. The image above also contains the patient's Facebook ID, which appears as the "c_user" ID highlighted above.[21]

68. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' Facebook IDs, IP addresses, and/or device IDs or other the information they input into Defendant's website, like their home address, zipcode, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[22] The Plaintiff's and Class Members identities could be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

[21] To preserve the Facebook users' anonymity, the c_user ID has been partially redacted.
[22] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Nov. 14, 2022)

69. The Facebook Pixel also intercepts and transmits information that patients type into search boxes, e.g., "do I have covid" or forms that request confidential information like patient contact information, medical histories, insurance and financial information, and Social Security numbers.

70. For example, the image below depicts what happens when a patient types the phrase "I have female incontinence" into the Website's search bar:

71. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, Facebook will associate the information with the visitor's Facebook ID and corresponding Facebook profile, i.e., their real-world identity.

72. A user's Facebook Profile ID is linked to their Facebook profile, which generally

contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

Defendant's Privacy Policies and Promises

73. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep Private Information private and confidential and they will only disclose Private Information under certain circumstances. [23]

74. Defendant publishes several privacy policies that represent to patients and visitors to its website that Defendant will keep sensitive information confidential and that they will only disclose PII and PHI provided to it under certain circumstances, none of which apply here.

75. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiff's and Class Members' Private Information in the following ways:

- To provide healthcare treatment to you;
- To obtain payment for services;
- For healthcare operations;
- To assist with joint healthcare operations;
- To remind you about appointments;
- To tell you about treatment options;

[23]https://www.ssmhealth.com/privacy-notices-terms-of-use/notice-privacy-practices (last visited: December 18, 2022).

- For health-related benefits and services;
- For patient assistance programs;
- For fundraising activities;
- For individuals involved in patient care or payment for patient care;
- For research;
- As required by law;
- For organ, eye, or tissue donation purposes;
- For military purposes;
- For worker compensation purposes;
- For law enforcement purposes;
- To coroners, medical examiner, & funeral directors;
- For national security & intelligence activities;
- For protective services for the president and others; and
- To a correctional institution, if applicable.

76. Defendant's Privacy Policy does not permit Defendant to intercept and disclose Plaintiff's and Class Members' Private Information to third-parties, including Facebook, for marketing purposes.

77. Defendant's Privacy Policy acknowledges Defendant is required by law to maintain the confidentiality of Plaintiff's and Class Members' Private Information, subject to the exceptions listed above.[24]

78. Defendant's Privacy Policy does not permit Defendant to use and disclose

[24] https://www.ssmhealth.com/privacy-notices-terms-of-use/notice-privacy-practices (last visited: December 18, 2022).

Plaintiff's and Class Members' Private Information for marketing purposes.[25]

79. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

Defendant Violated HIPAA Standards

80. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[26]

81. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

82. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[27]

83. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written

[25] *Id.*
[26] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[27] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022)

> authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[28]

84. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[29]

85. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

86. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Facebook Pixel.

Defendant Violated Industry Standards

87. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

88. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

89. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

[28] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)
[29] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

90. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

91. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

Plaintiff's and Class Members' Expectation of Privacy

92. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

93. Indeed, at all times when Plaintiff and Class Members provided their PII and PHI to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

IP Addresses are Personally Identifiable Information

94. On information and belief, through the use of the Facebook Pixel on the Defendant's Website, Defendant also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' Computer IP addresses.

95. An IP address is a number that identifies the address of a device connected to the Internet.

96. IP addresses are used to identify and route communications on the Internet.

97. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

98. Facebook tracks every IP address ever associated with a Facebook user.

99. Google also tracks IP addresses associated with Internet users.

100. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

101. Under HIPAA, an IP address is considered personally identifiable information:

a. HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

102. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

103. The sole purpose of the use of the Facebook Pixel on Defendant's website was marketing and profits.

104. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient

marketing on Facebook.

105. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

106. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

107. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

Plaintiff John Doe's Experience

108. Plaintiff entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff disclosed his Private Information to Defendant.

109. Plaintiff accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction.

110. Plaintiff reasonably expected that his communications with Defendant via the website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

111. Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

112. As described herein, Defendant worked along with Facebook and otherwise assisted and enabled Facebook with intercepting Plaintiff's highly sensitive communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

113. Defendant transmitted to Facebook Plaintiff's Private Information.

114. By doing so without Plaintiff's consent, Defendant breached Plaintiff's right to

privacy and unlawfully disclosed Plaintiff's Private Information.

115. Defendant did not inform Plaintiff that it had shared his Private Information with Facebook.

116. Plaintiff suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

117. Plaintiff has a continuing interesting in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

TOLLING

118. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that Plaintiff's PII and PHI was intercepted and unlawfully disclosed because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

119. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

120. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Facebook Pixel on Defendant's website and patient portal.**

121. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any

successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

122. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

123. Numerosity, Fed R. Civ. P. 23(a)(1). The Nationwide Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant's records.

124. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiff and Class Members to Facebook, Meta, and/or additional third parties.

d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their PII and PHI.

125. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

126. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

127. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an

appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

128. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

129. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that

experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

130. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

131. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

132. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

133. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

134. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

135. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the National Class)

136. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

137. The Private Information of Plaintiff and Class Members consist of private and confidential facts and information that were never intended to be shared beyond private communications.

138. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

139. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

140. The unauthorized disclosure and/or acquisition by a third party of Plaintiff's and Class Members' Private Information via the use of the Facebook Pixel by Defendant is highly offensive to a reasonable person.

141. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

142. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

143. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it incorporated the Facebook Pixel into its website because it knew the functionality and purpose of the Facebook Pixel.

144. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its website and encouraged patients to use that website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

145. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class Members was disclosed to a third party without

authorization, causing Plaintiff and the Class to suffer damages.

146. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

147. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

148. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

149. Plaintiff, on behalf of himself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII and PHI and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II
Violation of Missouri's Merchandising Practices Act
Mo. Rev. Stat. § 407.010 *et seq.*
(On Behalf of Plaintiff and the National Class)

150. Plaintiff repeats and re-alleges each and every paragraph in the Complaint as if fully set forth herein.

151. Plaintiff brings this claim individually and on behalf of the Class against Defendant.

152. The Missouri Merchandising Practice Act protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

153. The MMPA makes unlawful the "act, use or employment by any person of any deception, fraud, false pretense, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

154. Plaintiff, individually and on behalf of the Class, is entitled to bring this action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who visits, purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.020, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award to the prevailing party attorney's fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper.

155. Defendant is a "person" within the meaning of the Mo. Rev. Stat. § 407.010(5) in that Defendant is a domestic "not-for-profit corporation."

156. Plaintiff and members of the Class are "persons" under the MMPA in that they are natural persons who used Defendant's Website to obtain medical treatment and services.

157. The MMPA applies to Defendant's conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

158. The MMPA defines "merchandise" as any objects, wares, goods, commodities, intangibles, real estate, or services. *See* Mo. Rev. Stat. § 407.010. Thus, the medical

treatment sought by Plaintiff and Class Members qualifies as "merchandise" within the meaning of the Act. Additionally, the Website is a service which is used by Defendant in connection with the sale or advertisement of any merchandise in trade or commerce.

159. "Trade" or "commerce" is defined as "the advertising, offering for sale, sale, or distribution, or any combination thereof, of any services and any property, tangible or intangible, real, personal, or mixed, and any other article, commodity, or thing of value wherever situated." True Value's advertising, offering for sale, and sale of its search engine and the merchandise located thereon on www.truevalue.com is considered "trade" or "commerce" in the State of Missouri within the meaning of Mo. Rev. Stat. § 407.010(7).

160. The Missouri Attorney General has promulgated regulations defining the meaning of unfair practice as used in the above statute. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) An unfair practice is any practice which—

(A) Either—

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

(2) Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (*See, Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts,

sections 364 and 365).

161. Pursuant to Mo. Rev. Stat. §407.020 and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendant's acts and omissions fall within the meaning of "unfair."

162. Missouri case law provides that the MMPA's "literal words cover *every practice imaginable and every unfairness to whatever degree*." *Conway v. CitiMortgage, Inc.*, 438 S.W.3d 410, 416 (Mo. 2014) (quoting *Ports Petroleum Co., Inc. of Ohio v. Nixon*, 37 S.W.3d237, 240 (Mo. banc 2001). Furthermore, the statute's "plain and ordinary meaning of the words themselves . . . are unrestricted, all-encompassing and exceedingly broad." *Id.* at 240.

163. Defendant violated the MMPA by omitting and/or concealing material facts about its Website. Specifically, Defendant omitted and/or concealed that it disclosed Plaintiff's and Class Members' communications to/from Defendant regarding Private Information.

164. Defendant's direction and employment of the tracking Pixel and its disclosure to Facebook are material to its business. Defendant did not disclose to Plaintiff and Class Members that their Private Information would be disclosed to Facebook. Had Plaintiff and Class Members known that the tracking Pixel was embedded in the Website, they would not have used Defendant's Website.

165. Defendant intentionally concealed the interception, collection, and disclosure of website visitors' communications in the Website because it knows that Plaintiff and Class Members would not have otherwise used its Website. Indeed, Defendant's concealment of such facts was intended to mislead consumers.

166. Defendant's concealment, suppression, and/or omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

167. By failing to disclose and inform Plaintiff and Class Members about its interception, collection, and disclosure of Plaintiff's and Class Members' Website communications, Defendant engaged in acts and practices that constitute unlawful practices in violation of Mo. Ann. Stat. §§ 407.010, *et seq.*

168. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and Class Members have suffered actual harm in the form of money and/or property because the disclosure of their Private Information has value. The collection and use of this information has now diminished the value of such information to Plaintiff and the Class.

169. As such, Plaintiff and the Class seek an order (1) requiring Defendant to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs. Plaintiff and the Class seek all relief available under Mo. Ann. Stat. § 407.020, which prohibits "the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce…," as further interpreted by Mo. Code Regs. Ann. tit. 15, §§ 60-7.010, *et seq.*, Mo. Code Regs. Ann. tit. 15, §§ 60-8.010, *et seq.*, and Mo. Code Regs. Ann. tit. 15, §§ 60-9.010, *et seq.*, and Mo. Ann. Stat. § 407.025, which provides for the relief sought in this count.

170. Defendant's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class Members any time they utilize Defendant's Website. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the National Class)

171. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

172. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

173. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

174. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

175. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Missouri and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

176. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the National Class)

177. Plaintiff repeats and re-alleges each and every allegation contained in the

Complaint as if fully set forth herein.

178. When Plaintiff and Class Members provided their user data to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

179. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

180. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

181. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to a third party, *i.e.*, Facebook.

182. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

183. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq*.
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the National Class)

184. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

185. The ECPA protects both sending and receipt of communications.

186. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

187. The transmissions of Plaintiff's PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

188. **Electronic Communications**. The transmission of PII and PHI between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within he meaning of 18 U.S.C. § 2510(2).

189. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

190. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

191. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers;

d. Defendant's Website; and

e. The Pixel Code deployed by Defendant to effectuate the sending and acquisition of patient communications

192. By utilizing and embedding the Pixel on its website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

193. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook.

194. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

195. By intentionally disclosing or endeavoring to disclose the electronic communications of the Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

196. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

197. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

198. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

199. Defendant was not acting under color of law to intercept Plaintiff and the Class Member's wire or electronic communication.

200. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

201. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

202. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of Mo. Rev. Stat. § 407.010 *et seq*.

COUNT VI
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE 18 U.S.C. § 2511(3)(a) (On Behalf of Plaintiff and the National Class)

203. Plaintiff repeats and re-alleges each and every allegation contained in the

Complaint as if fully set forth herein.

204. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

205. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

206. Defendant's Website is an electronic communication services. Both services provide to users thereof the ability to send or receive electronic communications. In the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiff's and Class Members' PII and PHI.

207. **Intentional Divulgence**. Defendant intentionally designed the Pixel tracking and was or should have been aware that, if misconfigured, it could divulge Plaintiff's and Class Members' PII and PHI.

208. **While in Transmission**. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

209. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiff's and Class Members' communications to Facebook without Plaintiff's and Class Members' consent and/or authorization.

210. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication"

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

18 U.S.C. § 2511(3)(b).

211. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

212. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

213. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

214. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

215. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

216. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

217. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VII
VIOLATION OF
TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2702, *et seq.*
(STORED COMMUNICATIONS ACT)
(On Behalf of Plaintiff and the National Class)

218. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

219. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

220. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

221. Defendant intentionally procures and embeds various Plaintiff's PII and PHI through the Pixel Code used on Defendant's Website, which qualifies as an Electronic Communication Service.

222. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

223. Defendant stores the content of Plaintiff's and Class Members' communications on Defendant's Website and files associated with it.

224. When Plaintiff or Class Member makes a Website communication, the content of that communication is immediately placed into storage.

225. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through the Pixel Code.

226. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

e. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

f. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

g. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

h. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

i. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

j. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

k. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

l. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

m. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

227. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

228. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

229. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property

> of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

230. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

231. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

232. Defendant's divulgence of the contents of user communications on Defendant's Website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

233. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

234. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

235. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's

fee and other litigation costs reasonably incurred.

COUNT VIII
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, ET SEQ.
(On Behalf of Plaintiff and the National Class)

236. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

237. The Plaintiff's and the Class's mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

238. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

239. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class's private and personally identifiable data and content – including the website visitor's electronic communications with the website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications") which were never intended for public consumption.

240. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiff and the Class being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

241. Accordingly, Plaintiff and the Class are entitled to "maintain a civil action

against the violator to obtain compensatory damages and injunctive relief or other equitable relief."18 U.S.C. § 1030(g).

COUNT IX
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the National Class)

353. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

354. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

355. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

356. Plaintiff's and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its privacy policy.

357. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Facebook Pixel to disclose and transmit Plaintiff's Private Information and the contents of their communications exchanged with Defendant to third parties.

358. The third-party recipients included, but were not limited to, Facebook.

359. Defendant's disclosures of Plaintiff's and Class members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

360. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

361. As a direct and proximate cause of Defendant's unauthorized disclosures of patient

personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. General damages for invasion of their rights in an amount to be determined by a jury;

d. Nominal damages for each independent violation;

e. Defendant took something of value from Plaintiff and Class members and derived benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without compensating Plaintiff for the data;

f. Plaintiff and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

g. Defendant's actions diminished the value of Plaintiff's and Class members' Personal Information; and

h. Defendant's actions violated the property rights Plaintiff and Class members have in their Personal Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members:

D. For an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

DATE: January 4, 2023

Respectfully Submitted,

/s/ Tiffany Marko Yiatras
Tiffany Marko Yiatras, MOED Bar No. 58197MO
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: tiffany@consumerprotectionlegal.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Bryan L. Bleichner*

Philip J. Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon*
The Lyon Law Firm
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiff and the Putative Class

* *pro hac vice* forthcoming